


[Subscribe](#) (Full Service) [Register](#) (Limited Service, Free) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

(negotiating or matchmaking) and encryption and (bnf gramm



THE ACM DIGITAL LIBRARY

[Feedback](#) [Report a problem](#) [Satis](#)

Terms used:

negotiating or **matchmaking** and **encryption** and **bnf grammar** and **anonymous** and **secret** and **agreement** or **agent** and **broker** and **BNF**

 Sort results by

 Display results
[Save results to a Binder](#)
[Search Tips](#)
☐ Open results in a new window

 Try an [Advanced Search](#)

 Try this search in [The](#)

Results 121 - 140 of 200

 Result page: [previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

121 [ITiCSE 2001 working group reports: Resources for instructors of capstone courses in com](#)



Tony Clear, Michael Goldweber, Frank H. Young, Paul M. Leidig, Kirk Scott

 December 2001 **Working group reports from ITiCSE on Innovation and technology in comp education ITiCSE-WGR '01**

Publisher: ACM Press

 Full text available: [pdf\(2.17 MB\)](#)

 Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

Most computing programs now have some form of integrative or capstone course in which students complete a significant project under supervision. There are many different models for such courses and choosing the best model for a course is a complex task. This report is intended to assist instructors of capstone courses, particularly in the model of teaching and learning inherent in the capstone course. This paper discusses important issues that should be addressed when conducting capstone courses. The ...

122 [Secure key agreement for group communications](#)

Wen-Her Yang, Shih-Pyng Shieh

 November 2001 **International Journal of Network Management**, Volume 11 Issue 6

Publisher: John Wiley & Sons, Inc.

 Full text available: [pdf\(174.68 KB\)](#)

 Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

A secure key agreement protocol for group communications is proposed in this paper, which ensures the authenticity of group members and the privacy of group messages, and provides the properties of forward secrecy and backward privacy. In a group session, the common key is collaboratively established by all members. The overhead of key agreement is balanced among group members.

123 [Untrusted hosts and confidentiality: secure program partitioning](#)



Steve Zdancewic, Lantian Zheng, Nathaniel Nystrom, Andrew C. Myers

 October 2001 **ACM SIGOPS Operating Systems Review, Proceedings of the eighteenth ACM SIGOPS workshop on Operating systems principles SOSP '01**, Volume 35 Issue 5

Publisher: ACM Press

 Full text available: [pdf\(1.36 MB\)](#)

 Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

This paper presents secure program partitioning, a language-based technique for protecting code execution in distributed systems containing mutually untrusted hosts. Confidentiality and integrity are expressed by annotating programs with security types that constrain information flow; these programs are then automatically partitioned to run securely on heterogeneously trusted hosts. The resulting component programs collectively implement the original program.

124 [Session 3: discussion: Ontology in information security: a useful theoretical foundation and](#)



tool

Victor Raskin, Christian F. Hempelmann, Katrina E. Triezenberg, Sergei Nirenburg
September 2001 **Proceedings of the 2001 workshop on New security paradigms NSPW '01**

Publisher: ACM Press

Full text available: [pdf\(507.99 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

The paper introduces and advocates an ontological semantic approach to information security. Its ontology and lexicons, borrowed from the field of natural language processing, are adjusted to the needs of the new domain. The approach pursues the ultimate dual goals of including language data sources as an integral part of the overall data sources in information security and the specification of the information security community ...

Keywords: documentation, human factors, languages, security, standardization, theory

125 Computing curricula 2001



September 2001 **Journal on Educational Resources in Computing (JERIC)**

Publisher: ACM Press

Full text available: [pdf\(613.63 KB\)](#) [html](#)
(2.78 KB)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

126 The architecture and performance of security protocols in the ensemble group communication diamonds to guard the castle



August 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue

Publisher: ACM Press

Full text available: [pdf\(418.73 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

Ensemble is a Group Communication System built at Cornell and the Hebrew universities. It allows to create *process groups* within which scalable reliable fifo-ordered multicast and point-to-point communication are supported. The system also supports other communication properties, such as causal and total order, flow control, and the like. This article describes the security protocols and infrastructure of Ensemble using Ensemble with the extensions described ...

Keywords: Group communication, security

127 An optimally robust hybrid mix network



Markus Jakobsson, Ari Juels

August 2001 **Proceedings of the twentieth annual ACM symposium on Principles of distributed computing PODC '01**

Publisher: ACM Press

Full text available: [pdf\(858.02 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

We present a mix network that achieves efficient integration of public-key and symmetric-key cryptography. A *hybrid mix network* is capable of natural processing of arbitrarily long input elements, and is fast and asymptotically optimal in both senses. While the overhead in the size of input elements is linear in the number of elements, it is quite small in practice. In contrast to previous hybrid constructions, ours has optimal robustness against any minority coalition ...

128 Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world



Marjory S. Blumenthal, David D. Clark

August 2001 **ACM Transactions on Internet Technology (TOIT)**, Volume 1 Issue 1

Publisher: ACM Press

Full text available: [pdf\(176.33 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

This article looks at the Internet and the changing set of requirements for the Internet as it becomes commercial, more oriented toward the consumer, and used for a wider set of purposes. We discuss principles that have guided the design of the Internet, called the end-to-end arguments, and we discuss a risk that the range of new requirements now emerging could have the consequence of compromising the Internet's original design principles. Were ...

Keywords: ISP, Internet, end-to-end argument

129 SPINS: security protocols for sensor networks



Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar

July 2001

**Proceedings of the 7th annual international conference on Mobile computing
MobiCom '01**

Publisher: ACM Press

Full text available: [pdf\(242.17 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index](#)

As sensor networks edge closer towards wide-spread deployment, security issues become a concern. Much research has focused on making sensor networks feasible and useful, and has not concerned

We present a suite of security building blocks optimized for resource-constrained environments for secure communication. SPINS has two secure building blocks: SNEP and TESLA. SNEP provides two important baseline security primitives: Data confidentiality ...

130 Efficient filtering in publish-subscribe systems using binary decision diagrams

Alexis Campailla, Sagar Chaki, Edmund Clarke, Somesh Jha, Helmut Veith

July 2001

Proceedings of the 23rd International Conference on Software Engineering I

Publisher: IEEE Computer Society

Full text available: [pdf\(225.86 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

Implicit invocation or publish-subscribe has become an important architectural style for large-scale systems and evolution. The publish-subscribe style facilitates developing large-scale systems by composing developed components because the style permits loose coupling between various components. A major bottleneck in using publish-subscribe systems for very large scale systems is the efficiency of message matching, i.e., matching of published events with ...

131 Agent mediated electronic commerce research at Hewlett Packard Labs, Bristol



Chris Preist

June 2001

ACM SIGecom Exchanges, Volume 2 Issue 3

Publisher: ACM Press

Full text available: [pdf\(151.18 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Agent technology is a key enabling component in bringing about Hewlett-Packard e-services. For this reason, HP Labs is making significant investments in research in this area. Work on agent technology includes agent-mediated B2B e-commerce, distributed agent-based personalization, agent-based bandwidth, automated auction design, mobile agents, user profiling and FIPA standardization activities. In this article, we describe our work on ...

132 Matchmaking among minimal agents without a facilitator



Elith Ogston, Stamatis Vassiliadis

May 2001

Proceedings of the fifth international conference on Autonomous agents AGE

Publisher: ACM Press

Full text available: [pdf\(333.25 KB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)


Multi-Agent Systems are a promising way of dealing with large complex problems. However, it is not clear how much complexity or pre-existing structure individual agents must have to allow them to work

effectively. In this paper, we ask to what extent agents with minimal resources, local communication directory service can solve a consumer-provider matchmaking problem. We are interested in if it is massively scalable and can be used with re ...

Keywords: agent architectures, matchmaking, middle agents, multi-agent collaboration, multi-

133 A formal approach to protocols and strategies for (legal) negotiation

 Guido Governatori, Marlon Dumas, Arthur H. M. ter Hofstede, Phillipa Oaks
May 2001 **Proceedings of the 8th international conference on Artificial intelligence and**
Publisher: ACM Press

Full text available:  [pdf\(145.01 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We propose a formal and executable framework for expressing protocols and strategies for automated negotiation. In this framework a party involved in a negotiation is represented through a software agent consisting of four modules: (i) a communication module which manages the interaction with the other agents; (ii) a reasoning module specified as a defeasible theory; and (iii) a knowledge base with control and the reasoning modules, while keeping track of the state of the negotiation.

Keywords: auctions, automated legal negotiation, defeasible logic, software agents

134 Improving the representation of legal case texts with information extraction methods


 Stefanie Brüninghaus, Kevin D. Ashley
May 2001 **Proceedings of the 8th international conference on Artificial intelligence and**
Publisher: ACM Press

Full text available:  [pdf\(188.30 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The prohibitive cost of assigning indices to textual cases is a major obstacle for the practical use of CBR systems supporting reasoning and arguing with cases. While progress has been made toward extracting facts from well-structured case texts or classifying case abstracts under Key Number concepts, this does not suffice for the complexity of indexing concepts in CBR systems.


In this paper, we lay out how a better example representation may facilitate classification and reasoning.


135 Agent-oriented technology in support of e-business

 Mike P. Papazoglou
April 2001 **Communications of the ACM**, Volume 44 Issue 4
Publisher: ACM Press

Full text available:  [pdf\(145.21 KB\)](#)  [html\(39.13 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

136 Natural language processing for information assurance and security: an overview and implementation


 Mikhail J. Atallah, Craig J. McDonough, Victor Raskin, Sergei Nirenburg
February 2001 **Proceedings of the 2000 workshop on New security paradigms NSPW '00**
Publisher: ACM Press

Full text available:  [pdf\(1.29 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

137 Multilateral security a concept and examples for balanced security

 Kai Rannenberg
February 2001 **Proceedings of the 2000 workshop on New security paradigms NSPW '00**

Publisher: ACM Press

Full text available:  [pdf\(1.05 MB\)](#)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Keywords: GSM, mobile communication, multilateral security, negotiation, privacy, protection, management, security management, simulation study

138 [Simple and fault-tolerant key agreement for dynamic collaborative groups](#)



Yongdae Kim, Adrian Perrig, Gene Tsudik

November 2000 **Proceedings of the 7th ACM conference on Computer and communications**

Publisher: ACM Press

Full text available:  [pdf\(319.01 KB\)](#)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

139 [Regulating service access and information release on the Web](#)



Piero Bonatti, Pierangela Samarati

November 2000 **Proceedings of the 7th ACM conference on Computer and communications**

Publisher: ACM Press

Full text available:  [pdf\(599.91 KB\)](#)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Keywords: access control, digital certificate, privacy

140 [Verifying security protocols with Brutus](#)



E. M. Clarke, S. Jha, W. Marrero

October 2000 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 19

Publisher: ACM Press

Full text available:  [pdf\(347.12 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Due to the rapid growth of the "Internet" and the "World Wide Web" security has become a very important issue in the design and implementation of software systems. Since security has become an important part of protocols in this domain has become very large. These protocols are very diverse in nature. If an architect wants to deploy some of these protocols in a system, they have to be sure that the properties of the protocols as dictated ...

Keywords: authentication and secure payment protocols, formal methods, model-checking

Results 121 - 140 of 200

Result page: [previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM,
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [RealPlayer](#)

[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [Gmail](#) [more ▾](#)

[Sign in](#)

[Google](#)

negotiating and matchmaking and (broker or a

Search

[Advanced Search](#)
[Preferences](#)

Try uppercase "**OR**" to search for either of two terms. [\[details\]](#)

The "**AND**" operator is unnecessary – we include all search terms by default. [\[details\]](#)

Web Results 1 - 10 of about **49,900** for **negotiating and matchmaking and (broker or agent) and encryption** :

Methods and apparatus for negotiating agreement over concealed ...

Negotiation according to protocols established by the **Broker** including the creation and exchange of **one-way encryption** keys, the transfer of encrypted ...

www.freepatentsonline.com/20070005962.html - 56k - [Cached](#) - [Similar pages](#)

[PDF] Web-service Based Human Resource Recruitment by Using Matchmaking ...

File Format: PDF/Adobe Acrobat

cient way of **matchmaking** Web services for job exchange, vacancy recruitment, and job tion with each other regarding the **encryption** information ...

doi.ieeecomputersociety.org/10.1109/EDOCW.2006.77 - [Similar pages](#)

ACM: Digital Library: Communications of the ACM

The term **broker agent** may be perceived as synonymous to what is also known in the ...

Confidentiality refers to the use of **encryption** for scrambling the ...

portal.acm.org/citation.cfm?doid=367211.367268 - [Similar pages](#)

[PDF] AGENT-ORIENTED TECHNOLOGY IN SUPPORT OF E-BUSINESS

File Format: PDF/Adobe Acrobat - [View as HTML](#)

negotiation agents that **negotiate** on behalf of a buyer. or a seller; billing **agents**;

Confidentiality refers to the use of **encryption** for ...

infolab.uvt.nl/pub/papazogloump-2001-68.pdf - [Similar pages](#)

[PDF] Agent-Based Mediated Service Negotiation

File Format: PDF/Adobe Acrobat

one-way offering mechanism known as bidding (different bidding protocols exist, **Agent** containers are stored using **encryption**, preventing unauthorized ...

www.iids.org/aigaion/indexempty.php?page=actionattachment&action=open&pub_id=229&location=mob... - [Similar pages](#)

[PS] A MATCHMAKING APPROACH FOR DISTRIBUTED POLICY SPECIFICATION AND ...

File Format: Adobe PostScript - [View as Text](#)

key **encryption**. Two kinds of certificates can be issued by a principal. Passing this **grammar** to the Break the Chain algorithm, **one** of the possible ...

www.cs.wisc.edu/condor/doc/ncoleman-dissert.ps - [Similar pages](#)

[PDF] Standardizing Agent Communication

File Format: PDF/Adobe Acrobat - [View as HTML](#)

must implement it in the agreed-upon way. **One** of the design criteria for KQML issues, e.g. authentication of **agents'** identities and **encryption** of ACL ...

www.flacp.fujitsulabs.com/~yannis/publications/springer2001b.pdf - [Similar pages](#)

[PDF] Management of heterogeneous networks with intelligent agents

File Format: PDF/Adobe Acrobat

encryption. However, agreement could not be reached NM **agent** may implement security in a way analogous. to the **one** found in legacy NM systems. ...

doi.wiley.com/10.1002/bltj.2194 - [Similar pages](#)

[PS] A Mobile **Agent** Architecture for Distributed Information Management

File Format: Adobe PostScript

It is interesting to note that **one way** of defining AI [artificial **Agents** where **encryption** algorithms, self-validation and the like can help to ensure ...
eprints.ecs.soton.ac.uk/849/05/thesis.ps.gz - [Similar pages](#)

E Business Vocabulary for Students

Each **one** is issued by a bank and represents a specified sum of real money. Developed to account for weaknesses in symmetric **encryption**, public key ...
www.eslincanada.com/englishlesson12.html - 46k - [Cached](#) - [Similar pages](#)

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) **Next**

Try [Google Desktop](#): search your computer as easily as you search the web.

negotiating and matchmaking and (t

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)